

The materials provided are for information only. Any recommendations are offered solely for your consideration, to the extent applicable to your circumstances.

DIR IR Redbook Training

Texas Information Security
Forum 2022 – Day Two
May 17, 2022, 1:00 p.m.
Meeting Room 2



Texas Department of Information Resources

Transforming How
Texas Government
Serves Texans

Welcome and Introductions

DIR Office of the Chief Information
Security Officer (OCISO)

Cybersecurity Incident Response Team
(CIRT)



Meet the Team!

Jeremy Wilson

Deputy CISO, Security Operations/CIRT

*** Andrew Campbell**

Cyber Incident Response Team, Team Lead

Dennis Brown

Cyber Incident Response Team, Senior Analyst

Orane Douglas

Cybersecurity Sharing and Analysis Specialist/
Cyber Incident Response Team, Analyst

Jonathan King

Statewide Cyber Resilience & Response Manager

Presentation Charge

Getting to Know you Question

- Would you rather fast forward seven days or rewind 30 days?

Incident Response Preparedness

- Training people
- Planning for response
- Testing equipment
- Conducting tabletops
- Hardening networks and implementing monitoring tools

Responding to a Security Incident

- Running forensics and investigating logs
- Reimaging endpoints and rebuilding servers
- Patching exploited vulnerabilities
- Restoring data from backups (hopefully)
- Shoring up defenses to prevent a follow-on attack

Presentation Charge



Known for his brilliance on the battlefield, Patton often had to make decisions based on limited information and time. But he knew to avoid “paralysis by analysis,” make a decision and execute it the best he could. Otherwise, the enemy might maneuver faster and beat him.

We Are The Mighty | By Team Might
[11 quotes that show the awesomeness of Gen. George Patton](#)

Training Objectives

Terminal Objective

At the end of this training, the participant will have the **resources, knowledge, and ability** to use the DIR Incident Response Team Redbook to **facilitate the creation of their own IR plan, processes, and procedures.**

Enabling Objectives

The participant will be better able to:

- Develop an initial incident response policy for their organization.
- Identify personnel to include in incident response planning and define their organization's team structure.
- Understand the incident response phases and the goals of each phase.
- Develop initial incident triage and notification thresholds.
- Implement the foundational concepts of continuous improvement.
- Identify cybersecurity incident response best practices and locate relevant state and federal resources/ guides.

Agenda

Module	Title
Module 1	Welcome and Introductions
Module 2	Introduction to the DIR Redbook
Module 3	Incident Response Policy, Team Structure, Membership, and Roles
Module 4	Process Overview and Response Phases
Module 5	Incident Triage and Notification Thresholds
Module 6	Services Restoration Priority and Inventory
Module 7	After Action Review and Post Incident Analysis
Module 8	Incident Response Best Practices
Module 9	Close Out

Introduction to the DIR Redbook

Module 2



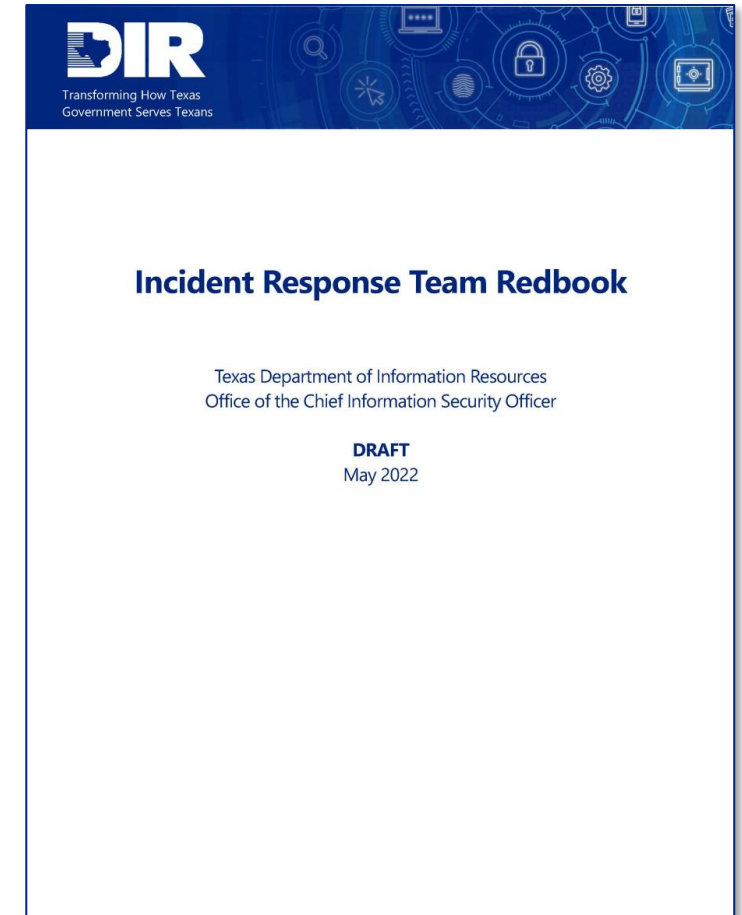
What is a Redbook?



What is a Redbook?

Multiple Resources in One

- Legal references for information security.
- Incident response team/ plan development guidance.
- Response and investigation contact and reference book.
- Cybersecurity program best practices and resources guide.
- And much more!



How do I use the IR Redbook?

As Reference

- Breach reporting legislation.

Table 4 Texas legal requirements for breach notices

Type	Citation	Requirement	Notes
Texas Identity Theft Enforcement and Protection Act (2019)	Business and Commerce Code section 521.053	Report any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person or to the data owner immediately. Public reports may be required	Gov't Code section 2054.1125 makes Business and Commerce Code 521.053 applicable to state agencies. Texas OAG Data

To Document Key Contacts

- Who to call and when during an incident.

Table 10 Contact Information Template

Entity or Organization	Title, Dept., or Location	Name	Phone	Email
Office of the Governor				
Texas State Representative				
Texas State Senator				
Chief Elected				

Tasks and Considerations

The framework is divided into five phases, which are listed in the graphic below. To support organizations just starting a cybersecurity program, the 'Setting up For Success' section includes some tasks and considerations that may help you initiate a program. To help maintain a program, the "Supporting Long-term Success" section has suggested tasks and considerations.



As a Starting Point

- Building a cybersecurity program.

What is our Intention for this Training?

Our Goals

- Provide guidelines to address common incident response issues.
- Share information relevant to incident response in the state of Texas.
- Provide a guide that is more consumable than the NIST Incident Handling Guide or a vendor template.

Our Caution

- The IR Redbook **is not a silver bullet**.
- Use these resources as a starting point and customize based on your organization's needs.
- For legal issues, coordinate with your organization's legal counsel.

Policy, Team Structure, Membership, and Roles

Module 3



Incident Response Policy

Purpose

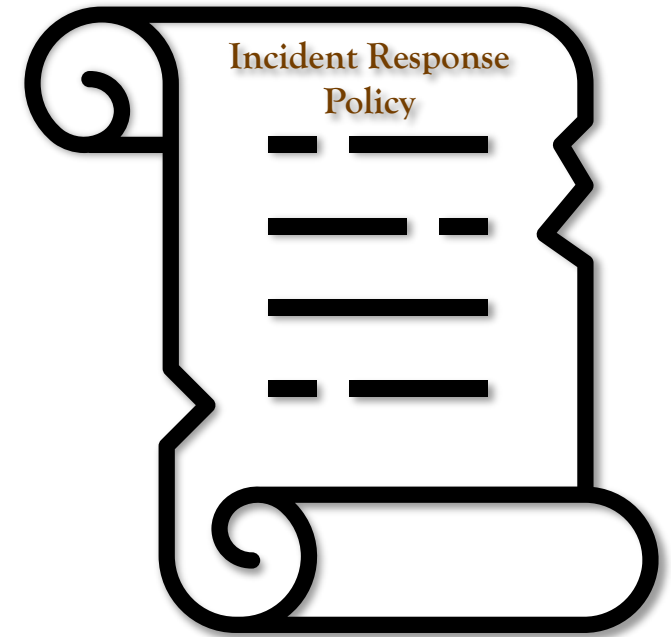
- Defines the expectations for incident management.
- Formalizes the response team structure.
- Documents delegations of authority.

Considerations

- Involve senior leadership in policy development.
- Formally adopt the policy.
- Review policy as appropriate.

Benefits

- Prompts response discussion before an incident occurs.
- Documents delegation of authority to support incident containment.
- Defines the organization's priorities.



Incident Response Policy

Where do you start?

- Texas Administrative Code (TAC) 202.
 - Required for state agencies, IHE, and public junior colleges.
 - Useful for local level organizations to review.

What's in a policy?

- Statement of management commitment.
- Scope of the incident response program.
- Participants in the incident response plan.
- Roles and responsibilities.
- Notification requirements.
- Other functions, based on organizational requirements.

Section	Guidance	
Purpose	The purpose of this Incident Response Policy is to establish a framework for identifying, containing, mitigating, and reporting privacy and security Incidents in accordance with Texas Administrative Code (TAC), Title 1, Chapter 202 . This document sets forth the policy for incident management within state level organizations but can be applicable to all organizations.	
Scope	<p>This policy applies to any computing device owned or leased by the organization.</p> <p>This policy applies to and must be complied with by all the organization's users. The user agrees to abide by this policy while employed or contracted with the organization.</p> <p>Roles and responsibilities of each function pertaining to the protection of organization-owned systems and data are documented in the organization's policy.</p> <p>The user is responsible for understanding the terms and conditions of this policy. Exemptions to this policy shall follow the process defined in organization policy.</p> <p>This policy is subject to change.</p> <p>This policy applies to any computing device owned or leased by the organization. It also applies to any computing device regardless of ownership, which either is used to store organization-owned confidential or organization-sensitive data or that, if lost, stolen, or compromised, and based on its privileged access, could lead to unauthorized data disclosure.</p>	
Policy	The Information Security Officer (ISO) is responsible for overseeing incident investigations in coordination with the Incident Response Team (IRT). The ISO shall recommend the IRT members to the Information Resources Manager (IRM) for approval.	1 TAC §202.26
	The highest priority of the ISO and IRT shall be to identify, contain, mitigate, and report privacy or security Incidents that	

Incident Response Policy

Policy Development Discussion

- Involve IT, business process owners, and other senior leaders.

Questions to Ask

- Who should be involved in planning/response?
- Is the entire organization covered by this policy?
- What are senior leadership's expectations for communication, recovery, and situational awareness.
- Does IT have authority delegated to take immediate protective action?

Incident Response Policy

The purpose of the [organization name] Incident Response Policy is to establish a framework and define requirements for addressing the impact of a security incident.

This policy applies to any computing device owned or leased by the organization, including cloud hosted systems as appropriate. Incident response roles and responsibilities are documented in the organization's response plan.

An incident response team [will be/is] established to respond to cyber incidents. This team consisting of individuals involved in decision making and prioritizing incident response activities.

The response team consists of personnel identified by the Leadership Team and documented in this Redbook with expertise in responding to a significant actual or suspected privacy or security event or incident. The response team operates on behalf of [Executive Management] and engages, informs, and receives support from [Executive Management].

There [is/is not] a set protocol to initiate the response team activities in response to an actual or suspected event/incident. Once activated, the response team has authority to [request cooperation/establish incident response priorities which may supersede daily business responsibilities or require attention outside normal business hours].

Incident Response Team Responsibilities

- **Anticipate and prepare** [organization name] for privacy or security events/incidents which can be reasonably anticipated.
- **Respond** to actual or suspected events/incidents on behalf of [organization name] as needed, with activities such as:





Team Structure, Membership, and Roles

Building an Incident Response Team

Who do you involve in IR planning?

- Technical staff
- Leadership
- Support staff

Building the Team

- Whole of organization approach.
- Incorporate members early in the process.
- Additional support may be needed during extended incident response activities.
- Nontraditional IT roles can become familiar with the incident response process.

Key Contacts

Organizations should establish an escalation process for instances when key individuals outside of normal technical response processes must be notified. Among those to be considered are:

- Chief Executive Officer (CEO), Director, Commissioner, or Chief (as applicable)
- Chief Information Officer (CIO) or Information Resources Manager (IRM)
- Chief Information Security Officer (CISO) or Information Security Officer (ISO)
- Chief Privacy Officer (CPO) or Privacy Officer
- Chief Risk Officer (CRO) or Risk Manager
- Other incident response teams within the organization
- External (contractor) incident response teams, if appropriate
- System owner
- Internal departments, including human resources, public affairs, and legal
- (Local) Mayor or County Judge
- (Local) Emergency Management Coordinator
- (Local) Texas Division of Emergency Management (TDEM) District Coordinator

Incident Response Team Structure

Purpose

- Keep people engaged and informed.
- Include representatives from different 'business' functions.
- Develop a manageable span of control.

Considerations

- Understand reporting structure of the organization.
- Education of information security may be required to improve engagement.

Benefits

- Improved communications.
- Pre-incident structure defined.
- Relationships established to support response activities.



Incident Response Team Structure

Leadership Team

Response Team Coordinator

Chief Elected Official

Executive Management

IT/Technology Directors

Legal

Communications

Core Team

IT Infrastructure

IT Applications

3rd party Security
Vendors

Other positions as needed

Extended Response Team

Human Resources

Facilities

Law Enforcement

Emergency Management

Additional Department Heads

Incident Response Team Structure

Leadership

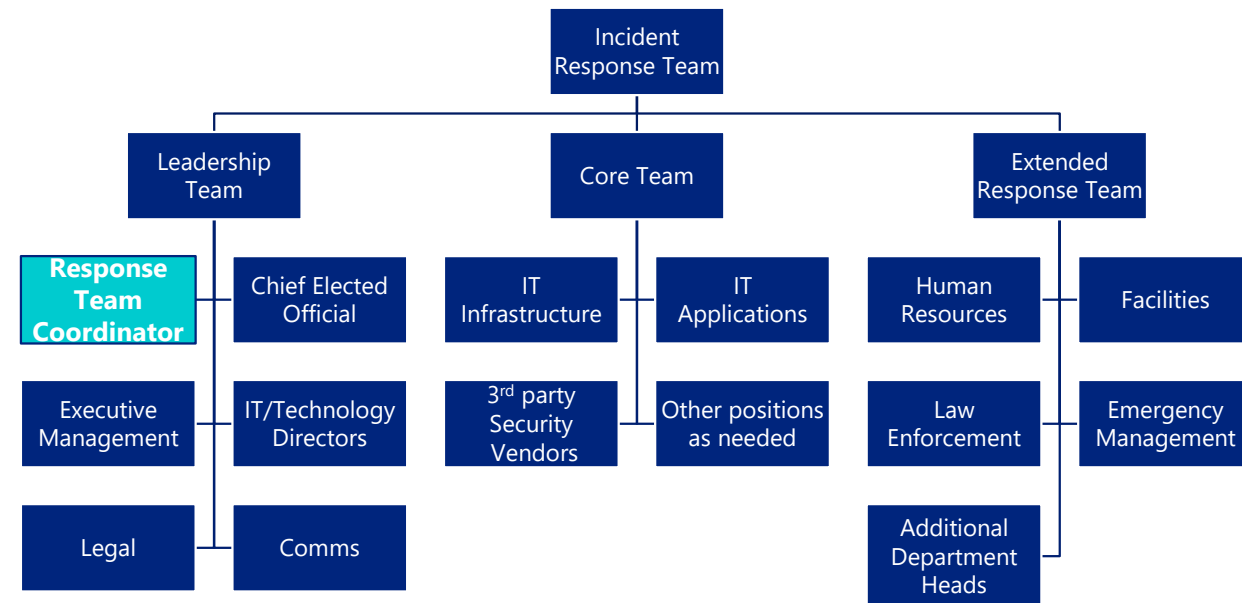
- Provides command objectives.
- Institutional knowledge.
- Decision making authority.

Core

- Facilitates activities to respond to a cybersecurity incident.
- Coordinates with response team members to implement command objectives.

Extended Response

- Provides unique subject matter expertise in their respective fields.





Team Membership and Roles

Sample Response Team Members

Incident Response
Team Coordinator

Chief Elected
Official

City Manager/
County
Administrator or
Superintendent

IT/ Technology
Director or
Information
Security Officer

Legal Counsel

Communications/
External Affairs

IT Infrastructure/
Applications
Manager

System/ Network
Administrators

Forensic or
Cybersecurity
Technicians/
Consultants

Human Resources

Law Enforcement

Emergency
Management

Finance/
Purchasing

Facilities

Other Roles as
Required

Sample Response Team Roles

Roles

- Redbook includes sample roles for each position.
- Customize roles based on team discussions.
- Capture high level functions.
- Remember to identify position, not an individual.
- Customize template to the needs of your organization.

Additional Guidance

- NIST Incident Handling Guide, Page 17, "Dependencies within Organizations"

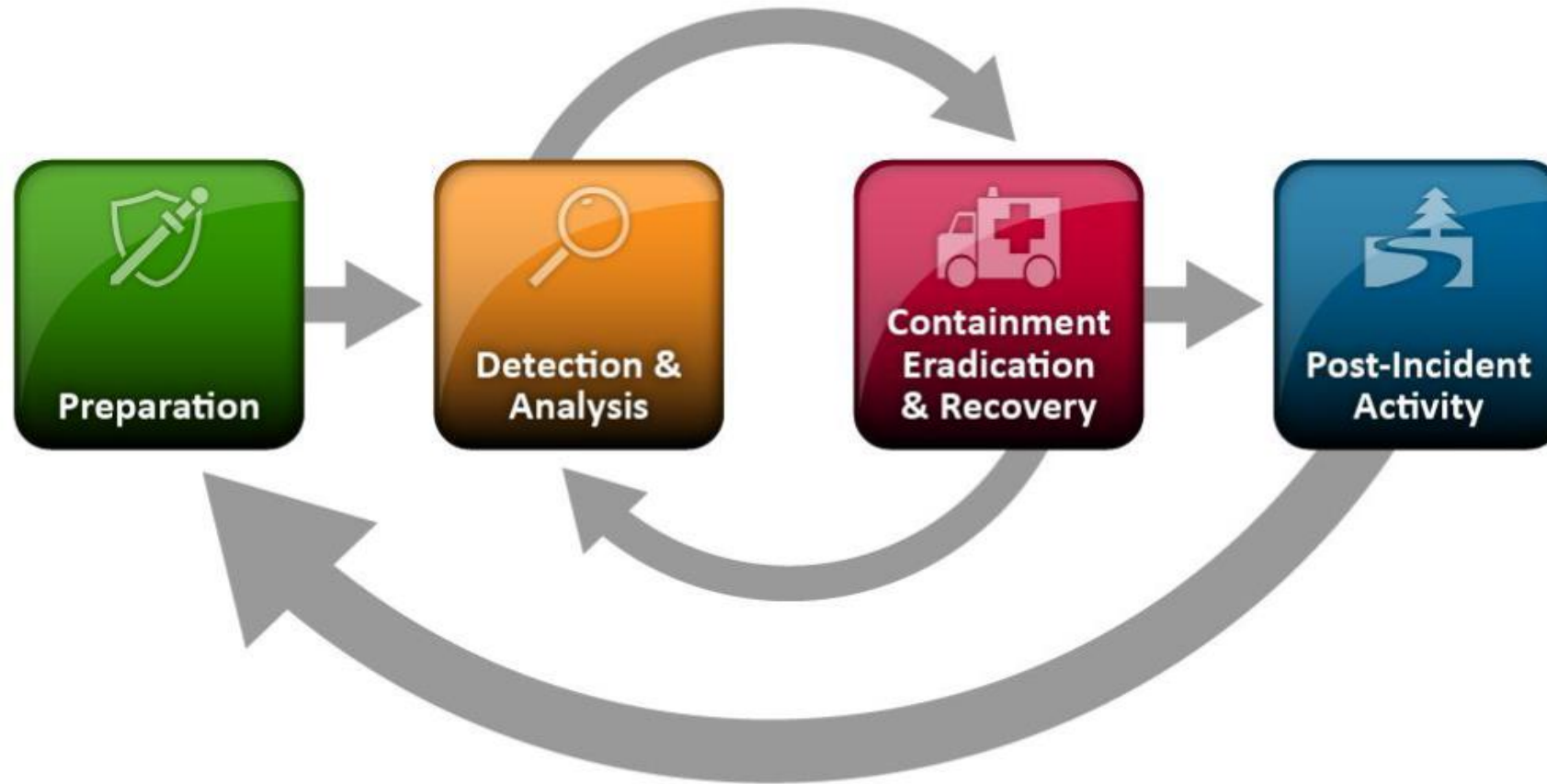
Table 8 Sample Team Member Roles		
Position	Team Component	Sample Roles
Incident Response Team Coordinator	Leadership	<p>The coordinator is identified by and reports to [Executive Management]. The coordinator manages all aspects of the response, coordinates communication, and ensures necessary notifications occur. The coordinator is the primary point-of-contact during the response. Their duties may include:</p> <ul style="list-style-type: none">- Incident triage and declaration.- Establish, maintain, and update written response team protocols or incident response plans.- Identify roles and responsibilities for response team members.- Request cooperation / establish event response priorities.- [Add additional duties based on organizational requirements]

Process Overview and Response Phases

Module 4



High Level Response Process Overview



NIST Incident Response Life Cycle

Incident Response Phase and Activity Sample

Phases

- Mirrors the NIST incident handling life cycle.

Description and Activities

- Provide the intent of each phase.
- Document specific activities for each phase.
- Progress may be cyclical.
- Response teams may need to step back to a previous phase.
- Activities don't need to be all encompassing.
- Reference external resources for additional guidance.

The table below outlines key activities and considerations during the incident response life cycle.

Table 11 Incident Response Phase and Activity Sample

Phase	Description and Activities
Preparation	<p>Incident response preparation activities may include establishing an incident response team, developing an incident response plan, and testing the plan and associated procedures. Preparation activities may also include increasing the resilience of systems, networks, applications, and backups to attack. Some common preparation activities include:</p> <ul style="list-style-type: none">• Establishing an incident response team.• Developing an incident response plan.• Preparing incident response resources.• Conducting user awareness and training activities.• Managing vulnerabilities and securing networks and systems.• [Add additional containment steps based on organizational requirements] <p>Additional preparation activities can be found on page 3 of the MS-ISAC/CISA Joint Ransomware Guide</p>

Incident Response Phases - Preparation

Goal

Increase the organization's readiness and resilience to a cybersecurity incident or attack.

Sample Steps

- Establishing an incident response team.
- Developing an incident response plan.
- Preparing incident response resources.
- Conducting user awareness and training activities.
- Managing vulnerabilities and securing networks and systems.



Incident Response Phases - Detection and Analysis

Goal

Determine if the observed event is a true cybersecurity incident and evaluate its severity.

Sample Steps

- Analyze precursors for signs of a potential attack.
- Analyze indicators to determine their potential impact.
- Review logs to coordinate potentially malicious events.
- Identify and triage an incident, determine its type and scope of impact.



Incident Response Phases - Containment

Goal

To limit further damage caused by an incident to reduce business impact to the organization.

Sample Steps

- System isolation.
- Disable services, protocols, or appliances.
- Disable account access.

*Each incident may require unique containment strategies. Preserving evidence and collecting forensic images and logs is a best practice to enable threat eradication.



PRO TIP

Keep systems powered on to preserve volatile memory, unless shutdown is required.

Incident Response Phases - Eradication

Goal

To eliminate the threat actor's persistence and address the vulnerability that allowed initial access.

Sample Steps

- Remediate or mitigate exploited vulnerabilities.
- Remove malware or other malicious files.
- Secure and reset compromised user accounts.



Incident Response Phases - Recovery

Goal

Restore systems to normal operation, confirm they perform as expected, and remediate remaining vulnerabilities.

Sample Steps

- Rebuild and reimage impacted workstation and servers.
- Sanitize user and service accounts.
- Segment network and review back up strategy.



Incident Response Phases - Post-Incident Activity

Goal

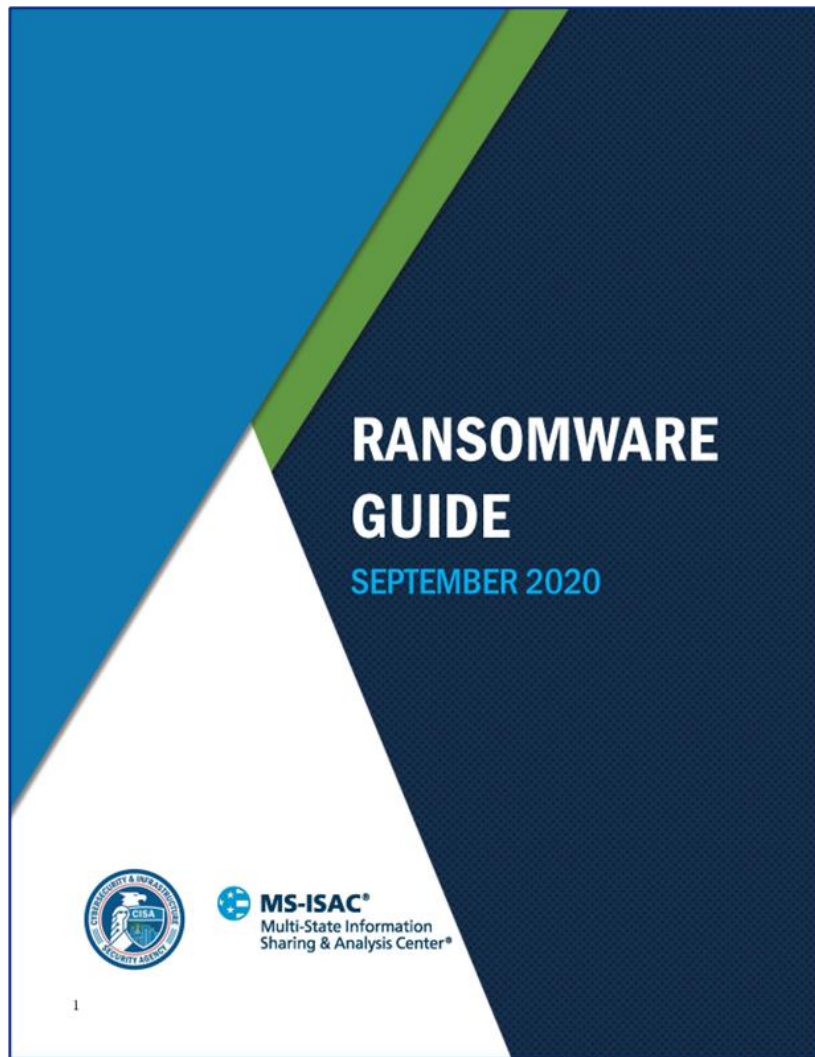
Improve incident response activities by working towards a cycle of continuous program improvement.

Sample Steps

- Recognize gaps, review policies and incident response plans, and identify corrective actions to address gaps.
- Consider opportunities to improve processes, coverage, and refine alerting of security tools.
- Conduct additional training for security and non-security staff.
- Review industry standards to ensure evidence retention requirements are met.



Incident Response Phases – Reference Resources



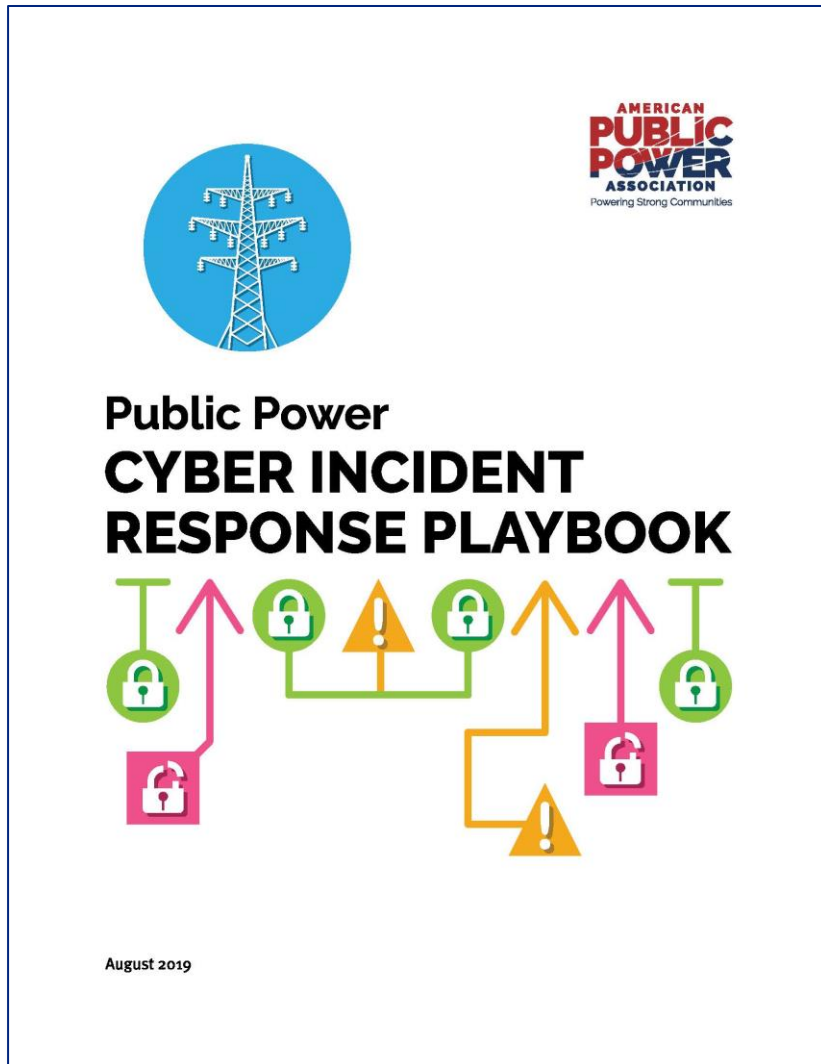
☐ 1. Determine which systems were impacted, and immediately isolate them.

- ☐ If several systems or subnets appear impacted, take the network offline at the switch level. It may not be feasible to disconnect individual systems during an incident.
- ☐ If taking the network temporarily offline is not immediately possible, locate the network (e.g., Ethernet) cable and unplug affected devices from the network or remove them from Wi-Fi to contain the infection.
- ☐ After an initial compromise, malicious actors may monitor your organization's activity or communications to understand if their actions have been detected. Be sure to isolate systems in a coordinated manner and use out-of-band communication methods like phone calls or other means to avoid tipping off actors that they have been discovered and that mitigation actions are being undertaken. Not doing so could cause actors to move laterally to preserve their access—already a common tactic—or deploy ransomware widely prior to networks being taken offline.

Note: Step 2 will prevent you from maintaining ransomware infection artifacts and potential evidence stored in volatile memory. It should be carried out **only** if it is not possible to temporarily shut down the network or disconnect affected hosts from the network using other means.

☐ 2. Only in the event you are unable to disconnect devices from the network, power them down to avoid further spread of the ransomware infection.

Incident Response Phases – Reference Resources



Enact Response Plan and Eradicate the Threat

Incident eradication should only be conducted after a complete investigation, and by an experienced team of cybersecurity experts. The CIRT should close any exposed vulnerabilities and remove the threat and any artifacts left by attackers (malicious code, data, etc.). This process should be rapid, thorough, and synchronized to avoid giving attackers time to cover their tracks or enact further damage. Eradication steps may include:

- Disabling breached user accounts and/or changing passwords
- Updating network intrusion detection system signatures to assess indicators of similar attacks in other parts of the environment
- Identifying exfiltrated data using packet capture (pcap) to assess network traffic
- Running a virus scanner to remove the compromised files or services
- Closing all network vectors of exfiltration and potential vectors for re-infection
- Informing employees of the threat or follow-up actions

Incident Triage and Notification Thresholds

Module 5



Incident Triage

Purpose

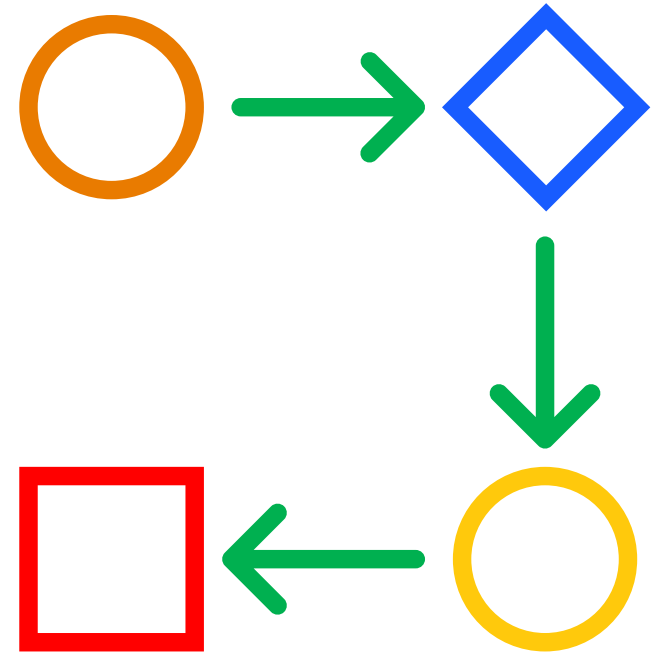
- To determine if an event or anomaly meets a predefined threshold to be classified as a cybersecurity incident.

Considerations

- Occurs as part of the 'detection and analysis' phase.
- Determine impact on business processes.
- Impacts are relevant to your organization.
- Triageed impacts may change as the incident evolves.

Benefits

- Thoroughly triaging an incident's impacts supports response resource and notification decisions.



Sample Incident Triage Template

Example Incidents Based on Level

4 Emergency

- Ransomware impacting all systems and backups with potential physical impacts.

3 High

- Ransomware impacting on-premises information systems.

2 Medium

- Denial of Service (DDOS) attack impacting critical business system.

1 Low

- Account compromise and associated phishing/ spam activity.

Customize the Incident Triage Template to fit the needs of your organization. For additional guidance, see *Table 1 Examples of Functional Impact Thresholds*.

Incidents will be assigned a severity tier based on the criteria defined below:

Level	Observed Functional Impacts					
	Impact Scope	Customer Impact	Continuity of Operations	Financial	Recoverability	Reputation
4: Emergency	Entire organization	Life safety systems impacted	Government services unavailable	Loss: \$Z+	Data lost and not recoverable	Significant risk for reputational harm
3: High	Multiple departments	Customer facing services inoperable	Department's services unavailable	Loss: \$Y - \$Z	Data lost but manually recoverable	Potential for reputational harm do to service outages
2: Medium	Multiple users	Customer facing services degraded	Single application unavailable	Loss: \$X - \$Y	Data lost but digitally recoverable	Limited potential for reputational harm
1: Low	Single user	No customer impact	No interruption	No Loss	No data lost	No harm

OCISO Cybersecurity Incident Thresholds

DIR Thresholds

- Aligns with the CISA National Cyber Incident Scoring System.
- Incidents are assigned a priority.
- Priority drives the response support and leadership notifications.

Threshold	Description
Catastrophic	<p>An incident meets the catastrophic threshold if it impacts multiple critical infrastructure systems or sectors including impacts to power generation and distribution, water and wastewater utilities, telecommunications, delivery of public health and medical services, government operations, public safety, or law enforcement information systems.</p> <p>Incident impacts may be noted across:</p> <ul style="list-style-type: none">- Multiple U.S. states, simultaneously- Multiple state agencies and/or jurisdictions
Emergency	<p>An incident meets the emergency threshold if it impacts a single critical infrastructure system, curtails delivery of public health and medical services, power generation and distribution, water and wastewater utilities, telecommunications, government operations, public safety services, receives national media attention, or federal government awareness. A local or state disaster declaration may be considered at this threshold.</p> <p>Incident impacts may be noted across:</p> <ul style="list-style-type: none">- Multiple local jurisdictions- Multiple state agencies- Multiple U.S. states, simultaneously
High	<p>An incident meets the high threshold if it results in noticeable impacts to government operations, public safety systems, reduces public confidence, receives media attention, or state legislative awareness.</p> <p>Incident impacts may be noted at:</p> <ul style="list-style-type: none">- A local jurisdiction- A state agency- Multiple U.S. states
Medium	<p>An incident meets the medium threshold if it results in the degradation of an organization's program or services, reduces public facing service delivery capacity, or receives minimal media or legislative attention.</p> <p>Incident impacts may be noted at:</p> <ul style="list-style-type: none">- A local jurisdiction- A state agency
Low	<p>An incident meets the low threshold if it impacts individual users or accounts.</p> <p>Impacts may be noted at:</p> <ul style="list-style-type: none">- A local jurisdiction- A state agency



Notification Thresholds

Notification Thresholds

Purpose

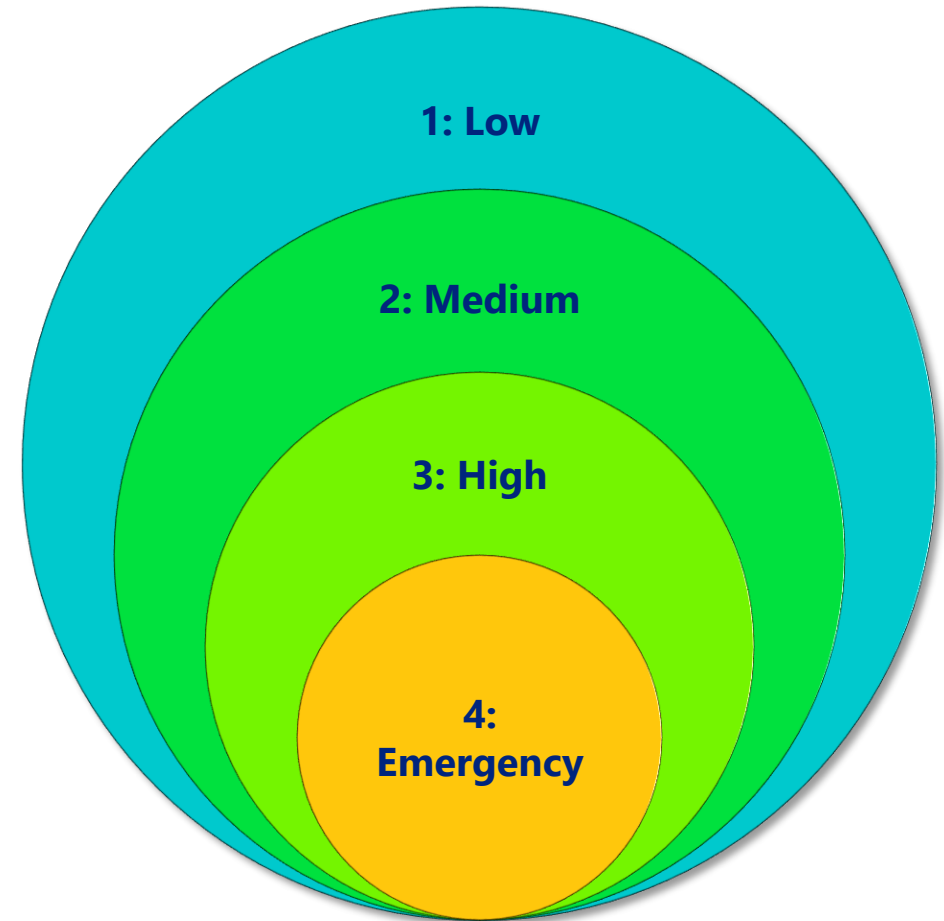
- Pre-identify which staff should be notified in case of a cybersecurity incident.

Considerations

- Coordinate with senior leadership to determine what notifications they want to receive.
- Incident triage may change and necessitate additional notifications.
- Consider adding external partners into thresholds discussion.

Benefits

- Reduced alert fatigue on senior leadership.
- Increased speed of critical information sharing.



Notification Thresholds Template

Sample Escalation Path

- Customize the escalation path based on discussion with response team members.
- Focus on notifying by position vs individual.
- Consider key criteria that require specific notifications, i.e., ransom note.
- Response team coordinator determines if 'considered notification' is required.

Table 16 Incident Notification Thresholds Template

Customize the Notification Escalation Path to fit the needs of your organization.

Level ³	Notification Escalation Path				
4: Emergency	Chief Elected Official	Council or Commissioners Court			
3: High	Legal Council	Human Resources	Public Information Officer	Emergency Management	Law Enforcement
2: Medium	Incident Coordinator	Incident Response Core Team	IT Director	City Manager (or equivalent)	
1: Low	Help Desk	IT Manager			
Color Key	Notification Recommended	Consider Notification			



OCISO Partner and Threshold Notifications

DIR Thresholds

- Developed with input from Executive Director and program leadership.
- Thresholds are synchronized across agency.
- Thresholds are reviewed and updated after major incidents.
- Additional document developed to identify who makes each notification decision and who makes requisite notification.

Partner	Low	Medium	High	Emergency	Catastrophic
State CISO	Informed	Informed	Informed	Informed	Informed
DIR Dep ED, COO, Public Affairs, and Media Director	Considered	Informed	Informed	Informed	Informed
DIR Executive Director		Considered	Informed	Informed	Informed
DIR Executive Leadership Team		Considered	Informed	Informed	Informed
Governor's Office		Considered	Informed	Informed	Informed
MS-ISAC and CISA		Considered	Considered	Informed	Informed
Law Enforcement (FBI)		Recommended	Recommended	Informed	Informed
Press Release			Considered	Informed	Informed
Social Media or Website Post		Considered	Considered	Informed	Informed
Texas ISAO Partners		Considered	Considered	Informed	Informed
Cybersecurity Council			Considered	Informed	Informed

Services Restoration Priority and Inventory

Module 6



Services Restoration Priority Worksheet

Purpose

- Pre-identify which systems are most critical to the organization's recovery.

Considerations

- Develop restoration priorities based on executive management's priorities.
- Include business process owners in discussion to set recovery exceptions.
- Evaluate system interdependencies in restoration prioritization.

Benefits

- Unified effort during the recovery phase.



Services Restoration Priority Worksheet

Priority Restoration Tiers

Tier 1

- Critical services or system and life safety or public safety systems.

Tier 2

- Core business functions and services that enable the operation of the entity.

Tier 3

- Routine business functions and services that support operations.

Tier 4

- Non-production services or functions that do not impact the end users.

Table 12 Services Restoration Policy Sample

The table below provides a consolidated list to guide service restoration.

Tier	Service/System	Function and Details	End User
1	Domain controllers	Authentication – Active Directory	Internal and External
1			
2			



Hardware and Software Inventory

Hardware and Software Inventory

Purpose

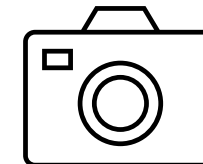
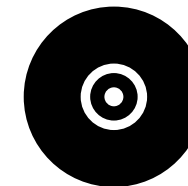
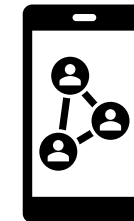
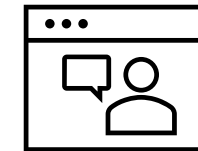
- Provides an authoritative record on organization's assets.

Considerations

- Include servers, network equipment, and IoT devices in inventory.
- Build inventory tracking process into existing onboarding/ offboarding process.
- Include a network typology diagram in inventory.

Benefits

- Provides a baseline for incident response and recovery activities.
- Supports a vulnerability management program.



Inventory Tracking Samples

Tracking Inventory

- Routinely refresh inventory
- Assign tracking function to appropriate business unit.
- Technological solutions may support tracking.

Supporting Resource

The Center for Internet Security (CIS) provides a hardware and software tracking spreadsheet sample.

Table 13 Hardware Tracking

Complete and maintain the following hardware asset tracking sheet. Customize headers as appropriate.

Asset Number	Current Status	Assigned Employee	Asset Type	Model	Manufacture	Serial Number	Location	Description	Date Issued/Returned
TX-###	Assigned	John Doe	Laptop	Model Name	Manufacture	XX###X	HQ Level 2	Main Device	xx/xx/xxxx

Table 14 Software Tracking

Complete and maintain the following software tracking sheet. Customize headers as appropriate.

Software Use	Name	Software Description	License Type	Version	Software Key	Date Purchased	Billing Cycle
End User	Adobe Lightroom	Photo Editor	Service	NA	In Console	xx/xx/xxxx	Billed Monthly

After Action Review and Post Incident Analysis

Module 7



After Action Review (AAR) and Improvement Process

Purpose

To allow incident response team to evolve, improve, and account for new threats, improved technology, and lessons learned from response.

Considerations

- A 'lessons learned' meeting with all involved parties should be conducted shortly after a major incident.
- Collect agenda items in advance to guide discussion.
- Avoid the 'blame game' by selecting a strong facilitator.

Benefits

- Continuous improvement of the incident response team.



Post-Incident Documentation

Templates Include

- Incident information
- Lessons learned questions
- Root cause analysis questions
- Response strengths
- Improvement opportunities

Facilitation Guidance

- Provide questions to guide discussion in lessons learned meetings.
- Develop a post incident survey.
- Include general staff members in survey opportunities.
- Capture what went well!

7.4 Post-Incident After Action Review and Improvement Plan

Incident Post-Incident After Action Review Template

Use the sections below to capture post-incident comments captured in a hot-wash or after-action review.

Table 18 Incident Information Template

[Replace the content in brackets with your own details and information.]

Item	Description
Cyber Incident	[Use your organization's naming convention for the incident.]
Dates and Times	[Indicate, at a minimum, the start/end dates/times of the incident. Include a full incident chronology if available.]
Description	[Give a brief description of the incident.]
Impact	[What was the impact to the organization?]
Detection	[How was the incident detected?]
Metrics	[Enter any related metrics e.g., mean-time-to-incident-discovery, cost of recovery, time from detection to containment, etc.]
Incident Costs	[What was the cost in time, materials, human resources, and lost productivity to the organization in dollar figures? These could range from time and resources, equipment replacement costs, organization downtime, idle employee time, backlog catchup overtime, etc.]

Corrective Action Plan

Documenting Corrective Actions

- Develop improvements and associated actions based on lessons learned discussions.
- Socialize recommendations with response team members and organizational leadership.
- Focus on actionable and attainable improvements.

Implementing the Action Plan

- Routinely follow-up with the identified stakeholders.
- Socialize changes to the response plan or procedures with all team members.

Table 23 Corrective Action Plan

This corrective action plan has been developed for [Organization] because of the [incident name] Cyber Incident.

Improvement	Corrective Action	Responsible Stakeholder	Start Date	End Date	Notes or Limitations
1. [Improvement One]	1.1 [Corrective Action]	[Name/Org]	MM/DD/YY	MM/DD/YY	[As Needed]
	1.2 [Corrective Action]				
	1.3 [Corrective Action]				
2. [Improvement Two]	2.1 [Corrective Action]				
	2.2 [Corrective Action]				
	2.3 [Corrective Action]				

Incident Response Best Practices

Module 8



Texas Cybersecurity Best Practices

Set up For Success

- Identify a cyber champion.

Identify

- Inventory systems and data.

Protect

- Provide security awareness training to end users.

Detect

- Enable malware protection.

Respond


- Develop an incident response plan.

Recover


- Develop and test business continuity/ recovery plan.

Support Success

- Engage with cyber community.




Office of the
**Chief Information
Security Officer**
State of Texas



How to Set Up a Successful Cybersecurity Program

Implementing a cybersecurity program is one of the best ways to protect your organization from cybersecurity threats.

 **Start by identifying a cyber champion.**
Gain leadership support to help build a culture of cyber awareness. Then, move into the five core functions of the Texas Cybersecurity Framework to address and manage cybersecurity risk: Identify, Protect, Detect, Respond, and Recover.

1 Identify

- Inventory systems and data.
- Perform a security assessment.

2 Protect

- Implement and test back-ups.
- Train end users on security awareness topics.

3 Detect


- Establish a vulnerability management process.
- Enable malware protection.

4 Respond

- Identify incident response partners.
- Develop and test an incident response plan.

5 Recover

- Develop and test a business continuity and disaster recovery plan.

 **Engage with the cybersecurity community to further mature your program.**

Get Started Here! <https://dir.texas.gov/information-security/cybersecurity-incident-management-and-reporting>

The DIR Redbook will provide more details:

The materials provided are for information only. Any recommendations are offered solely for your consideration, to the extent applicable to your circumstances. Any third-party views and opinions do not necessarily reflect those of DIR or its employees. By sharing this material, DIR does not endorse any particular person, entity, product or service.

Texas Department of Information Resources | dir.texas.gov | #DIRisIT | @TexasDIR

Best Practices for Incident Response

Identify

- Inventory systems and their associated data.
- Develop security policies and document processes.

Protect

- Implement, protect, and test back-ups and data.
- Evaluate cyber protection system's needs.

Detect

- Develop vulnerability management process.
- Enable malware protection.
- Establish a log retention and review process.

Response

- Develop incident response plan.
- Test incident response plan.
- Establish relationships with response partners.

Recover

- Develop disaster recovery and business continuity plan

Support Long-Term Success

- Establish an after-action report process.
- Consider conducting post-incident assessments.

Best Practices for Incident Response

Supporting Resources

- Includes free or low-cost options.
- Organized by phase of the Texas Cybersecurity Framework.

Contact DIR if you have further questions or would like to find out if your organization is eligible for DIR funded resources.

Supporting Resources

These resources are available free or at a reduced cost to support security program development.

Phase	Resource
Set-Up	Multi-State Information Sharing and Analysis Center (MS-ISAC) and the CIS Security Best Practice Team's First Steps Within a Cybersecurity Program
	Texas Cybersecurity Awareness Month Resources
Identify	Texas DIR Managed Security Services (MSS) - Risk and Compliance Services
	Texas Cybersecurity Framework
	CISA Cybersecurity Assessments and Technical Services
	Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Assessments and Technical Services – Cyber Hygiene: Vulnerability Scanning
	CISA Insights Risk Considerations for Managed Service Provider Customers
	Department of Homeland Security/MS-ISAC Nationwide Cybersecurity Review
	Center for Internet Security (CIS) Policy Template Guide and CIS Controls
	CIS Controls V8
	Conference of State Bank Supervisors Ransomware Self-Assessment Tool
Protect	Texas DIR Managed Security Services (MSS) - Security Monitoring and Device Management Services (SMDM)
	Texas DIR Statewide Cybersecurity Awareness Training Resources
	CISA and MS-ISAC Joint Ransomware Guide Part 1: Ransomware Prevention Best Practices
	Multi-State Information Sharing and Analysis Center (MS-ISAC) Malicious Domain Blocking and Reporting (MDBR) Service and other MS-ISAC Cybersecurity Services
	Center for Internet Security Cyber Market SANS Online Technical Training
	Federal Virtual Training Environment (FedVTE) Free Online Cybersecurity Training

Close Out

Module 9



Training Objectives

Terminal Objective

At the end of this training, the participant will have the **resources, knowledge, and ability** to use the DIR Incident Response Team Redbook to **facilitate the creation of their own IR plan, processes, or procedures.**

Enabling Objectives

The participant will be better able to:

- Develop an initial incident response **policy** for their organization.
- Identify **personnel** to include in incident response planning and define their organization's **team structure.**
- Understand the incident response **phases** and the **goals** of each phase.
- Develop initial incident **triage** and **notification thresholds.**
- Implement the foundational **concepts of continuous improvement.**
- Identify cybersecurity incident response **best practices** and locate relevant state and federal **resources/guides.**

Guiding Resources

Cybersecurity Incident Response and Preparedness Resources

- <https://dir.texas.gov/information-security/cybersecurity-incident-management-and-reporting>

Join the Texas Information Sharing and Analysis Organization (TX-ISAO)

- <https://dir.texas.gov/information-security/txisao>

Public Power Cyber Incident Response Playbook

- <https://www.publicpower.org/system/files/documents/Public-Power-Cyber-Incident-Response-Playbook.pdf>

CISA MS-ISAC Ransomware Guide

- https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf

Thank You

dir.texas.gov

#DIRisIT

@TexasDIR



Texas Department of Information Resources

Transforming How
Texas Government
Serves Texans